REMARKS

Claims 1 and 2 are cancelled without prejudice or disclaimer. New claims 3-31 have been added. Claims 3-31 are now pending in this application. Minor changes have been made to the specification, however, no new matter has been added.

SUMMARY

Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

If any fees are due in connection with the filing of this Amendment, the Commissioner is authorized to deduct such fees from the undersigned's Deposit Account No. 50-0388 (Order No. VISAP064). A duplicate copy of the transmittal sheet for this amendment is enclosed for this purpose.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Phillip P. Lee
Reg. No. 46,866

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
(650) 961-8300

Marked up Version of Specification and Claims

Changes made in the Specification

In a second embodiment, the invention is directed towards the use of an integrated circuit card (also known as a smart card or chip card). One aspect of the second embodiment pertains to a method for authenticating the **[identity of a cardholder utilizing a chip card]** **chip card being used by a customer**. This method involves verifying that said cardholder client device includes a chip card reader and then prompting said cardholder to enter said chip card into the chip card reader. After the chip card reader receives the chip card, the chip card generates a cryptogram which is then sent to the access control server. The access control server then independently generates a second cryptogram based upon information in the chip card and compares the chip card cryptogram to the second cryptogram. If the two independently generated cryptograms match, then the authenticity of the card is verified.

Please replace the pending paragraph, which begins on page 9, the 1st continuing paragraph with:

The issuer domain 102 includes an enrollment site 108, an issuer cardholder system 110, the cardholder client device 122, an enrollment server 112, an access control server 114, an issuer or third party identity authentication component 116, and an account holder file 118. Optionally, the issuer domain 102 can include an issuer file of approved cardholders 120. The enrollment server 112 is a computer that manages cardholder enrollment into the PAS service through presenting a series of questions via a web interface to be answered by the cardholder and verified by the issuer. As shown in FIG. 1, the card issuer operates the enrollment server 112. However, a service organization, such as Visa, may operate the enrollment server 112 on behalf of the issuer. The issuer may use a web-enabled, interactive "identity authentication service" provided by a third party during the enrollment process to help validate a cardholder's identity. The enrollment server 112 is connected via the Internet to the Internet Payment Gateway Service 124, which is in turn, connected to a telecommunications network 126, for example, VisaNet. The Internet Payment Gateway Service 124 allows the enrollment server 112 to communicate with the telecommunications network 126. The connection via the Payment Gateway Service 124 allows the enrollment server 112 to query the issuer's authorization system **[127]** **138** to

determine if a cardholder being enrolled has an active card account. Enrollment site 108 is an Internet web site where the cardholder can register to participate in the PAS.

Please replace the pending paragraph, which begins on page 12, the 2nd full paragraph with:

Before an Issuer can be set up to use PAS they must obtain a **[copy o fall]** **copy of all** PAS software specified in the Issuer domain and install hardware systems and the PAS software. Then, Issuer financial institutions will also provide identity authentication policies and participating BIN information to PAS to be used in cardholder identity verification processes. Optionally, the issuer can provide to the PAS the cardholder authentication information for pre-loading into the account holder file 118. Pre-loading facilitates large volume support of cardholders. For example, when an issuer desires to activate all or most of its cardholders for PAS, the issuer can send PIN numbers to all of its cardholders. The PIN number can then be used by each cardholder to access his or her preloaded passwords. In this manner, the enrollment process is expedited because each cardholder need not go through the formal PAS enrollment process. After the cardholders use their preloaded password for the first time, the cardholders have the option of designating a new and easier to remember password.

Please replace the pending paragraph, which begins on page 15, the 2nd full paragraph with:

On the other hand, if the account number is determined to be within a range of account numbers present in directory server 128, then the second step of the verification process begins. The second step of the verification begins by the directory sending the ACS capable of authenticating the cardholder the card number to determine if the card is enrolled. If the card is not enrolled, the enrollment process is terminated. If the ACS indicates that the card is enrolled, the ACS via the directory server returns its URL Internet address to the merchant plug-in. The merchant plug-in then invokes the ACS via the cardholder client device and its resident browser. Once again it is noted that there can be multiple ACS's in PAS.

Please replace the pending paragraph, which begins on page 16, the 1st full paragraph with:

The payment authentication continues if the correct password is immediately entered or **[is]** **if** the correct response is provided by the cardholder to the hint question within the allowed number of attempts. The ACS then proceeds to digitally sign a receipt using the issuer's signature key or a service provider's key. This receipt will contain the merchant name, card account number, payment amount, and the payment date. The receipt file 130 stores the following transaction data: merchant name, merchant URL, card account number, expiration date, payment amount, payment date, the issuer payment signature and the cardholder authentication verification value. The ACS then redirects the cardholder back to the merchant plug-in through the cardholder browser. At this point, the ACS also passes to the merchant the digitally signed receipt and the determination as to whether the cardholder has been authenticated. The validation server 136, in the acquirer domain 106, is used by the merchant plug-in 134, to verify the digital signature used to sign the payment receipt. After verifying the digital signature, the cardholder is deemed "authenticated." In some embodiments of the invention, after the transaction is completed, the cardholder will also have the ability to re-register his or her card account and create a new password to be used for future online purchases.

Please replace the pending paragraph, which begins on page 21, the start of the 3rd paragraph with:

In the case that the acquirer domain 106 contains a validation server, the validation server 136 validates the signature on the *PARes*. The validation server 136 then returns the result of the signature validation to the merchant plug-in. **[If the signature cannot be validated, merchant plug-in notifies the merchant that the transaction cannot be treated as a PAS transaction.]** On the other hand, if the signature is validated, the merchant proceeds with an authenticated payment authorization. The *PARes* message may also be passed from the merchant to its acquirer payment processor 140 as shown in line 6a. The *PARes* message may then be passed from the acquirer through a telecommunications network 142 to the issuer. Thus, the payer authentication results are made available to the issuer as part of the standard payment authorization process.

Please replace the pending paragraph, which begins on page 25, the start of the 3rd full paragraph with:

In a second technique, the PAS password is automatically supplied to the ACS by the chip card. This technique uses passwords stored on the chip card to authenticate the cardholder in order to allow the cardholder to utilize the chip card. This approach uses an applet resident on the card referred to as the "Access" applet, because it provides universal access to the card**[,]** and its resident applications, and can be used to authenticate a cardholder. The Access applet can also disable access to the applications on the card. Upon presentation of the single, universal "Access" password and authentication of the cardholder, the Access applet then allows the cardholder to access to a variety of services or applications (e.g., access to an online banking site, access to an electronic bill payment service). For example, by presentation of a single "Access" password, the applet then allows use of any stored passwords on the card.

Please replace the pending paragraph, which begins on page 25, the start of the last paragraph with:

Generally, the set up procedures and the authentication process for the chip card embodiment are the same as for the traditional card embodiment. The differences between the chip card embodiment and the traditional **[chip]** card embodiment will be evident in the description that follows.

Please replace the pending paragraph, which begins on page 26, the 2nd full paragraph with:

FIG. 10A provides a high-level system architecture view of one embodiment of the chip card payer authorization service. As usual, the payment transaction begins when the cardholder accesses a merchant's electronic commerce web site using a cardholder client device 122. The cardholder client device 122 **contains a chip payer authentication client plug-in 1542 and** is connected to the issuer access control server 114, which has a chip payer authentication ACS plug-in 115. The issuer ACS 114 is connected to an account holder file 118, which is in turn connected to a receipt file 130. The merchant 132 uses a merchant plug-in software module 134 to participate in the payer authentication service. The merchant 132 is connected to the directory server 128, the validation server 136, and the acquirer payment processor 182. The acquirer payment processor 182 is connected to the payment network 126, which is in turn connected to the issuer 180.

Please replace the pending paragraph, which begins on page 27, the 3rd full paragraph with:

Now, FIG. 12 is presented to illustrate payment process flows that are superimposed upon a chip card system architecture according to one embodiment of the present invention. The chip card authentication architecture 1500 involves the cardholder client device 1510, the issuer's ACS 1520, the cardholder 1530, the chip card 1540, and the requesting party 1550. The requesting party in the PAS environment is typically the merchant. The cardholder client device 1510 includes a display device 1512, terminal software 1514, PIN pad or key entry device 1516, and the card reader 1518. The card reader **[1528]** **1518** is the electromechanical device into which a chip card is inserted for use with a terminal application, functionally equivalent to a Card Acceptance Device or InterFace Device (IFD in a physical point of sale environment).

Please replace the pending paragraph, which begins on page 30, the 3rd paragraph, line 16 with:

This section briefly describes the phases of the VSDC Authentication processing in the order in which they occur as illustrated in **[the preceding diagram]** **FIG. 12A**:

842 312

Changes in the Claims:

1. (Cancelled)

2. (Cancelled)

3. A payment authentication system that supports a payment authentication service wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, the system comprising:

an issuer domain including

an access control server being configured to receive and verify a password from said customer, said access control server also configured to sign a transaction receipt using a digital signature key and to send the digitally signed transaction receipt to said third party,

an account holder database controlled by said trusted party, said account holder database containing a list of customer accounts that are enrolled with said payment authentication service,

an enrollment server configured to control the enrollment of customer accounts into the payment authentication service, and

an enrollment Internet web site at which enrolling customers enter information in order to enroll with the payment authentication service;

an acquirer domain including

a third-party server, and

a third-party plug-in software module contained within said server of said third party, said module configured to send a payment request message to said access control server, said payment request message prompting said access control server to request said password from said customer; and

an interoperability domain including

a receipt database that is configured to store receipts for authenticated purchase transactions.

4. A payment authentication system that supports a payment authentication service wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, the system comprising:

an access control server controlled by said trusted party, said access control server being configured to receive and verify a password from said customer, said access control server also configured to sign a transaction receipt using a digital signature key and to send the digitally signed transaction receipt to said third party;

an account holder database controlled by said trusted party, said account holder database containing a list of customer accounts that are enrolled with said payment authentication service; and

a third-party plug-in software module contained within a server of said third party, said module configured to send a payment request message to said access control server, said payment request message prompting said access control server to request said password from said customer.

5. A payment authentication system as recited in claim 4, further comprising a directory, said directory containing ranges of customer account numbers that are associated with issuer financial institutions participating in said payment authentication service.

6. A payment authentication system as recited in claim 4, further comprising:

an enrollment server configured to control the enrollment of customer accounts into the payment authentication service; and

an enrollment Internet web site at which enrolling customers enter information in order to enroll with the payment authentication service.

7. A method wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:

requesting, by said trusted party from said customer, of an identity authenticating password;

verifying, by said trusted party, that said identity authenticating password from said customer matches a password previously designated for said account; and

notifying a third party, by said trusted party, that said customer is the actual owner of said account when said identity authenticating password entered by said customer matches the password that was previously designated for said account, whereby said notified third party desires verification as to the identity of said customer before proceeding with an online transaction with said customer.

8. A method as recited in claim 7 wherein said trusted party is an issuer financial institution and said third party is an online merchant, whereby said online merchant conducts a financial transaction with said customer, and wherein said account of said customer is maintained by said issuer financial institution.

9. A method as recited in claim 7 further comprising:

querying an access control server to determine if an account of said customer is enrolled in a payment authentication service.

10. A method as recited in claim 9 wherein the access control server determines if said customer account is enrolled by verifying that said customer account is contained in a database of enrolled customer accounts.

11. A method as recited in claim 9 further comprising:

querying a directory server to verify that said customer account is associated with an issuer financial institution that is participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

12. A method as recited in claim 11 further comprising:

sending to said third party's computer system an Internet address for said access control

server, said Internet address passing through said directory server before reaching said third party's computer system, whereby said Internet address for said access control server allows said third party to directly communicate with said access control server.

13. A method as recited in claim 9 further comprising:

reviewing a memory device controlled by said third party to verify that said customer account is associated with an issuer financial institution participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution.

14. A method as recited in claim 7 further comprising:

generating, by said trusted party, a digitally signed transaction receipt using a signature key of said trusted party; and

sending, by said trusted party, of a digitally signed transaction receipt to said third party, whereby the digitally signed transaction receipt confirms to said third party that the identity of said customer has been authenticated.

15. A method as recited in claim 14 wherein said transaction receipt includes a number associated with said customer account, a transaction payment amount, and a transaction payment date.

16. A method as recited in claim 7 further comprising:

sending, by said trusted party, of a card authentication verification value to said third party, the card authentication verification value containing a unique value for said customer account and a specific payment transaction, whereby said card authentication verification value uniquely identifies a specific authenticated payment transaction.

17. A method as recited in claim 8 further comprising:

verifying, by said third party, of said digitally signed transaction receipt such that said third party is assured that said transaction receipt was sent from a specific trusted party.

18. A method as recited in claim 7 further comprising:

sending, by said third party, of an authorization message to an issuer financial institution to verify said customer account has adequate credit for a requested purchase.

19. A method as recited in claim 7 wherein said customer enrolls in said payment authentication service, the method further comprising:

receiving, by said trusted party, of enrollment information entered at an enrollment Internet web site by said customer;

verifying, by said trusted party, that said enrollment information substantially matches information contained within a pre-existing database of customer information; and

storing said customer account information in a database for enrolled customer accounts.

20. A method performed by a payment authentication service wherein a trusted party authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:

sending a payment request message to a customer software module from a third-party software module;

receiving a payment request message at an access control server that is operated by said trusted party, said payment request message being sent to said access control server from said customer software module;

requesting, by said trusted party, of a password from said customer;

verifying, by said trusted party, that said password entered by said customer is valid; and

sending, by said trusted party, a payment response message to a third-party software module, said payment response message containing an authentication status indicator.

21. A customer software module containing computer code used with a payment

authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said customer software module effecting the following:

receiving a payment request message from a third party that requests the initiation of a payment authentication service wherein the identity of a customer will be authenticated;

sending said payment request message to an access control server operated by said issuer financial institution, said customer having an account with said issuer financial institution; and

receiving a request from said access control server for said customer to enter a password used to verify the identity of said customer.

22. A third-party computer used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said third-party computer comprising:

an Internet web page configured to present and receive information from said customer;

a plug-in software module configured to send a payment request message to a customer software module, said payment request message causing an access control server to query said customer for a password, said third-party plug-in software module configured to receive a payment response message which contains an authentication status, said authentication status serving to inform said third-party computer system whether or not the identity of said customer has been authenticated; and

a payment database for storing said authentication status, transaction data and payment data.

23. A method performed by an enrollment server used with a payment authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction is the actual owner of said account, said method comprising:

supporting an enrollment Internet web page to present and receive information from a customer for the purpose of enrolling said customer into said payment authentication service;

presenting questions to said customer intended to illicit answers from said customer useful for verifying the identity of said customer;

if the identity of said customer is verified, providing a customer software module to a customer client system, said customer software module containing computer code that will allow said customer to participate in said payment authentication service.

24. A method wherein a trusted party authenticates, for the benefit of a third party, that a customer using chip card during an online transaction has possession of the actual chip card issued to said customer, said method comprising:

receiving, at an access control server operated by said trusted party, a chip card cryptogram generated by said chip card based upon information in said chip card;

independently generating a second cryptogram by said access control server, said second cryptogram generated based upon information sent to said access control server from a customer client device;

comparing, at said access control server, the chip card cryptogram to the second cryptogram to determine whether or not said customer is utilizing a chip card that was previously issued to said customer; and

sending, from said access control server, of a payment response message to said third-party in order to notify said third-party whether or not said chip card has been authenticated.

25. A method as recited in claim 24 wherein said access control server is operated by a financial institution that issued said chip card to said customer.

26. A method as recited in claim 24 further comprising:

verifying that said customer client device includes a chip card reader; and

prompting said customer to insert said chip card into said chip card reader, whereby insertion of said chip card allows for communication between said chip card and said chip card reader.

27. A method as recited in claim 24 further comprising:

receiving, at said trusted party, of a password entered by said customer, said password being received at said access control server; and

verifying, by said trusted party, of said password to authenticate the identity of said customer, said password being verified by said access control server.

28. A method as recited in claim 24 further comprising:

verifying that said customer is enrolled in said payment authentication service; and

sending a payment request message to an access control server, said payment request message containing information necessary for said chip card to generate said chip card cryptogram.

29. A method as recited in claim 24 further comprising:

receiving a universal access password by said chip card, said universal access password sent by said customer;

unlocking a second password by using said universal access password, said second password contained within an access application resident on said chip card; and

accessing one or more chip card applications and their respective passwords by using said second password, said chip card applications being resident on said chip card.

30. A method as recited in claim 29 wherein one of the chip card applications is a debit and credit payment application that can be used in a payment type transaction.

31. A method as recited in claim 30 further comprising:

sending a password for said debit and credit payment application to said access control server; and

verifying said password to authenticate the identity of said customer, said password being verified by said access control server.